doi:10.11959/j.issn.1000-436x.2016147

无线网络中基于无证书聚合签名的高效匿名漫游认证方案

刘丹，石润华，张顺，仲红
（安徽大学计算机科学与技术学院，安徽 合肥 230601）

摘 要：针对无线移动网络漫游认证中的隐私保护需求，提出了新的匿名漫游认证方案。引入在线离线签名技术，并巧妙结合聚合验证方法，设计了一个无证书聚合签名方案。与相关方案相比，该签名方案降低了签名和验证过程的计算开销，提高了通信效率。继而，基于该签名方案，提出了一种新型高效的匿名漫游认证方案，简化了传统的三方漫游认证模型。理论分析结果表明，该方案安全、有效，特别适用于大规模无线移动网络。
关键词：无线移动网络；无证书；聚合；漫游认证；隐私保护
中图分类号：TP309,TP393 **文献标识码**：A

Efficient anonymous roaming authentication scheme using certificateless aggregate signature in wireless network

LIU Dan, SHI Run-hua, ZHANG Shun, ZHONG Hong
(School of Computer Science and Technology, Anhui University, Hefei 230601, China)

Abstract: To solve the privacy-preserving problem during the roaming authentication of wireless mobile networks, a novel roaming authentication scheme with anonymity was presented. An efficient certificateless aggregate signature scheme was first constructed, by introducing the online/offline signature and combining the aggregate signature. Compared with the related schemes, the proposed scheme has higher efficiency in computations of both signature and verification, and also improves the efficiency in communications. Furthermore, based on the proposed signature scheme, a novel roaming authentication scheme with anonymity was presented, in which it simplified the traditional three-party authentication model. The theoretical analysis shows that this scheme is secure and effective, and thus it is especially suitable for large-scale wireless mobile networks.
Key words: wireless mobile network, certificateless, aggregate, roaming authentication, privacy-preserving

1 引言

随着移动通信和网络技术的快速发展，无线网络作为传统有线网络的扩展，不仅得到了广泛的应用，也给人们带来了极大的便利。因其特殊的组网方式，在设计无线网络安全协议时需要考虑的安全问题更多，所以，大部分有线网络中的安全协议是不适合无线网络的。

漫游是无线网络中的关键服务之一。漫游服务固然方便，但安全问题不能忽视，尤其是在接入认证时可能会出现用户的真实身份、位置遭到泄露等情况。移动用户在外地网络请求服务时，对用户来说，他希望自己的真实身份、位置等信息能得到相应的保护，可以采用匿名漫游认证的方法，防止恶

收稿日期：2015-11-03；**修回日期**：2016-05-02
通信作者：张顺，shzhang27@163.com
基金项目：国家自然科学基金资助项目(No.61173187, No.61572001, No.11301002)；国家教育部博士点基金资助项目(No.20133401110004)；安徽省自然科学基金资助项目(No.1408085QF107)；安徽省高校省级优秀青年人才基金重点基金资助项目(No.2013SQRL006ZD)；安徽大学“211”基金资助项目(No.17110099)
Foundation Items: The National Natural Science Foundation of China (No.61173187, No.61572001, No.11301002), PhD Programs Foundation of Ministry of Education of China (No.20133401110004), The Natural Science Foundation of Anhui Province (No.1408085QF107), Talents Youth Fund of Anhui Province Universities (No.2013SQRL006ZD), 211 Project of Anhui University (No.17110099)

意的攻击者窃取这些隐私信息；而对外地服务器来说，首先要检验用户的合法性，然后去判断是否给予服务，从而避免非法用户请求服务，造成服务资源浪费。可见，用户的隐匿性和不可追踪性对漫游认证来说尤为重要。

为此，本文构造了一个安全、有效的基于无证书的聚合签名方案，不仅解决了证书开销和密钥托管问题，还将签名过程分为在线和离线这 2 个阶段，降低了签名和验证过程所需计算开销，提高了通信效率，使协议在计算和存储能力受限的移动环境下具有可用性。另外，在漫游认证中采用聚合签名技术，将多个签名聚合成一个签名，只需对聚合后的签名进行验证便可知签名是否合法，提高了验证效率。简而言之，本文的方案能够实现移动用户在不暴露自己真实身份的前提下安全地进行漫游认证。

2　相关工作

最近有关无线网络中漫游认证的研究，大多数方案运用各种密码技术设计不同方法来解决安全和隐私这 2 大挑战性问题，但出现了一些不可避免的安全漏洞。基于对称密钥的方法[1~6]，要求任意 2 个服务器之间预先建立对称密钥，这使管理复杂、成本高、可扩展性差。而基于 PKI 的方法[2,7~13]虽然具有较好的可扩展性，但证书开销带来了额外的计算开销和通信代价。为解决证书开销问题，引入基于 ID-PKC 的方法[14~17]，大大简化了证书的管理，但也存在不可忽视的安全缺陷。

另外，在漫游认证过程中，按照参与方的不同，可分成三方漫游认证和两方漫游认证。三方漫游认证简单模型如图 1 所示。2005 年，田子建等[18]设计了一种环签名方法来实现匿名认证。2009 年，Hou 等[19]构造了一种基于组合公钥的接入认证方法，实现了用户身份的隐匿性。2012 年，Zhang 等[20]采用一种基于无证书的公钥密码体制（CL-PKC, certificateless public key cryptography）的方法，解决了密钥托管的问题，但方案中家乡代理（HA, home agent）却知道移动节点（MN, mobile node）和外地代理（FA, foreign agent）之间的会话密钥，不具有安全性。上述方案都是采用三方漫游认证的方法，不具有统一性，而两方漫游认证具有统一性的特点，较好地避免了针对 HA 的拒绝服务（DoS, denial of service）攻击，其简单模型如图 2 所示。2010 年，Yang 等[17]设计了一种基于群签名（GS, group signature）的认证方法，采用假名技术实现强用户隐匿性，并基于撤销令牌实现动态撤销的性质。He 等[21]也设计了基于群签名的认证方法，实现强用户隐匿性和隐私保护性，并指出文献[17]的不足之处，遗憾的是，该方案不满足不可追踪性。Yang 等[17]还设计了一种基于 ID-PKC 的认证方法，但 FA 能获取用户的真实身份，不能保证强用户隐匿性。He 等[22,23]证明了 Yang[17]和 He[20]方法不能满足条件隐私保护。综上所述，三方漫游认证和两方漫游认证这 2 类方法在隐私保护方面仍旧存在某些安全漏洞，所以本文要找到最合适的方法，达到具有隐私保护性、统一性的漫游认证。

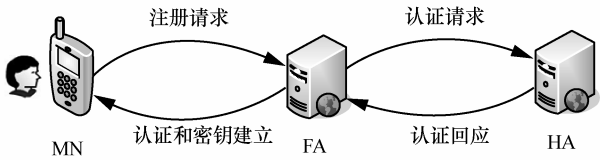

图 1　三方漫游认证简单模型

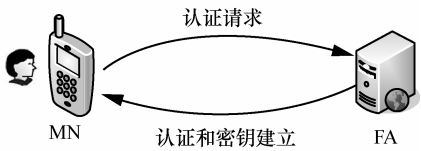

图 2　两方漫游认证简单模型

除了安全和隐私，效率也是不可忽略的重要问题。基于 PKI 的认证方法不可避免对证书的管理，证书传输和验证使通信代价大大提高。基于 ID-PKC 的认证方法虽然解决了证书管理带来的开销问题，却不能避免双线性对的运算开销。基于群签名的认证方法使用撤销密钥来实现用户的动态撤销，但当网络中的用户数量不断增长，验证开销也随之提高。三方漫游认证方法必须要求 HA 和 FA 至少交互一次才能完成认证。而在一般情况下，HA 为远程服务器，会带来很大的通信代价。

依据上述详细分析，可见现有大多数方案无论是在安全、隐私方面，还是在效率方面都存在一些问题，本文要保证漫游认证在安全、高效的情况下，注重隐私保护的实现。本文基于无证书的聚合签名（CLAS, certificateless aggregate signature）[27~29]方法，实现了具有隐私保护性、统一性的匿名漫游认证。在安全和隐私方面，本文的方案解决了密钥托管问题，避免了 DoS 攻击；采用预装载别名技术，实现了强用户隐匿性和不可追踪性；通过在别名后

附加有效期限，实现了用户的动态撤销；将用户真实身份与别名绑定在一起，实现了条件隐私保护。在效率方面，本文采用具有统一性的两方漫游认证方法，仅在 MN 与服务器 FA 之间进行；方案中 MN 没有耗时的双线性对操作，计算开销小；服务器 FA 利用聚合签名技术，能够一次验证多个 MN 签名，大大减少了验证时间。

3 系统模型

在本文的漫游认证方案中，系统模型主要由 3 个实体组成：MN、HA 和 FA，如图 3 所示。网络中有许多服务器，可以是 HA 或 FA；每个服务器管理一组需要订阅服务的用户，即 MN。

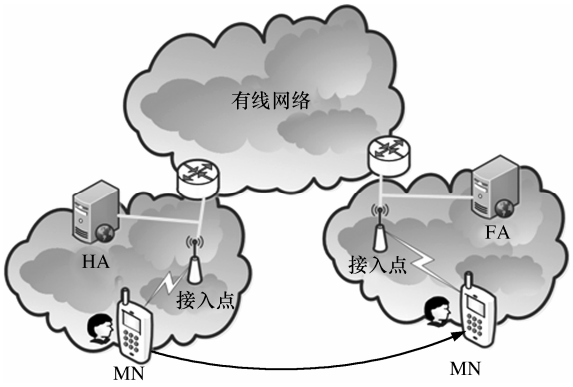

图 3 漫游认证系统模型

4 无证书聚合签名方案

本文提出了一个高效的无证书聚合签名方案，方案分别由以下 9 个算法组成。

1) 系统初始化算法（setup）

KGC 选择一个安全参数 $\lambda \in Z^+$，满足 $q > 2^\lambda$。G_1、G_2 是 2 个阶均为素数 q 的循环群，这 2 个循环群满足双线性对 $e: G_1 \times G_1 \to G_2$，其中，$G_1$ 是循环加法群，G_2 是循环乘法群，P 是 G_1 的生成元。KGC 选择一个随机数 $s \in_R Z_q^*$ 作为系统主密钥并计算

$$P_{\text{Pub}} = sP \tag{1}$$

然后挑选 3 个散列函数 $H_0: \{0,1\}^* \to G_1$、$H_1: \{0,1\}^* \to G_1$ 和 $H_2: \{0,1\}^* \to Z_q^*$。最后，KGC 公布系统参数 $params = \{\lambda, q, e, G_1, G_2, P, P_{\text{Pub}}, H_0, H_1, H_2\}$，秘密保存 s。

2) 部分私钥提取算法

首先，给定一个身份 ID_i，KGC 计算

$$D_i = sQ_i \tag{2}$$

并把它作为用户的部分私钥，其中，本文令 $Q_i = H_0(ID_i)$。随后 KGC 通过安全信道将 D_i 发送给用户 ID_i。

3) 秘密值生成算法

用户随机选取 $x_i \in_R Z_q^*$，作为其秘密值。

4) 私钥生成算法

用户的秘密值和部分私钥结合后，那么用户的最终私钥为 $sk_{ID_i} = (x_i, D_i)$。

5) 公钥生成算法

给定用户的私钥 (x_i, D_i)，用户计算

$$X_i = x_i P \tag{3}$$

并将 X_i 视为公钥。

6) 签名算法

本文将签名算法分为 2 个阶段：离线签名算法和在线签名算法。

离线签名：在没有收到消息之前，给定私钥 $sk_{ID_i} = (x_i, D_i)$，签名者随机选择 $r_i \in_R Z_q^*$，计算离线签名 (R_i, V_i, S_i)。

$$H = H_1(\Delta) \tag{4}$$

$$R_i = r_i P \tag{5}$$

$$V_i = r_i H \tag{6}$$

$$S_i = D_i + x_i H \tag{7}$$

其中，要注意的是用户选择相同的状态信息 Δ，这里 Δ 可以为空，也可以为某个系统公开参数，随机数或其他可用信息。

在线签名：给定一个消息 m_i 和离线签名，签名者计算在线签名。

$$h_i = H_2(m_i, ID_i, X_i, \Delta) \tag{8}$$

$$T_i = V_i + h_i S_i \tag{9}$$

那么得到的签名 $\sigma_i = (R_i, T_i)$ 就是用户 ID_i 对消息 m_i 的在线签名。

7) 单个验证算法

给定与身份 ID_i 有关的消息 m_i 的在线离线签名 σ_i，验证者计算

$$Q_i = H_0(ID_i) \tag{10}$$

$$H = H_1(\Delta) \tag{11}$$

$$h_i = H_2(m_i, ID_i, X_i, \Delta) \tag{12}$$

验证等式

$$e(P,T_i)=e(P_{\text{Pub}},h_iQ_i)e(H,R_i+h_iX_i) \quad (13)$$

是否成立，如果成立，则验证者接受此签名，反之拒绝。

8) 聚合算法

聚合者将一组不同的签名聚合后，形成一个聚合签名。

①给定一组用户集合 $U=\{U_1,U_2,\cdots,U_n\}$，每个用户 U_i 对应的身份为 ID_i，每个用户 U_i 对应的公钥为 X_i，以及相对应的消息签名对 $\{(m_1,\sigma_1=(R_1,T_1)),\cdots,(m_n,\sigma_n=(R_n,T_n))\}$。

②聚合者再计算

$$R=\sum_{i=1}^{n}R_i \quad (14)$$

$$T=\sum_{i=1}^{n}T_i \quad (15)$$

输出对消息 $m_1,m_2,\cdots,m_n$ 的聚合签名 (R,T)。

9) 聚合验证算法

给定系统公开参数、身份 ID_i、消息 m_i、公钥 X_i 以及聚合签名 (R,T)，验证者开始执行以下步骤来验证聚合签名。

①对于 $i=1,2,\cdots,n$，计算 $Q_i=H_0(ID_i)$。

②计算 $H=H_1(\Delta)$。

③对于 $i=1,2,\cdots,n$，计算 $h_i=H_2(m_i,ID_i,X_i,\Delta)$。

④对于聚合签名 (R,T)，验证等式

$$e(P,T)=e(P_{\text{Pub}},\sum_{i=1}^{n}h_iQ_i)e(H,R+\sum_{i=1}^{n}h_iX_i)) \quad (16)$$

是否成立，如果等式成立，输出“1”；否则输出“0”。

5　签名方案分析

5.1　安全模型和安全性分析

无证书聚合签名的安全模型中，包含 2 种类型的攻击者。

1) 第 1 类攻击者（即 A_1）是在不知道系统主密钥的情况下，可以替代用户的公钥。

2) 第 2 类攻击者（即 A_2）是在知道系统主密钥（恶意的 KGC）的情况下，生成用户的部分私钥，但此情况下不能替代用户的公钥。

文献[30]对攻击者类型 A_2 做了进一步改进，可获知系统主密钥，可替换除了目标用户之外的任何用户的公钥。

定理 1　在随机预言机模型和 CDH 困难假设下，本文方案在第 1 类攻击者 A_1 的适应性选择消息、选择身份以及公钥替换攻击下是存在不可伪造的。

引理 1　在随机预言机模型下，如果存在一个至多执行 $q_{H_i}(i=1,2)$ 次询问、q_{PPK} 次部分私钥查询、q_{SV} 次秘密值询问以及 q_{S} 次超级签名查询的类型敌手 A_1，他能够在时间 t 内以不可忽略的概率 ε 成功攻破本文的 CLAS 方案，那么存在一个这样的算法 C，能利用算法以概率 $\varepsilon'\geqslant\left(1-\frac{1}{q_C}\right)^{q_{\text{PPK}}+q_{\text{SV}}}\cdot\left(1-\frac{1}{q_{\text{S}}+1}\right)^{q_{\text{S}}}\frac{1}{(q_C(q_{\text{S}}+1))\varepsilon}$ 在时间 $t'<t+O(3q_C+q_{H_1}+q_{H_2}+4q_{\text{S}}+2n+1)t_{\text{m}}$ 内解决 CDH 问题，其中，t_{m} 表示一个点乘运算。

证明　给定一个随机的 CDH 问题实例 (P,aP,abP)，然后挑战者与敌手 A_1 进行交互。C 的目标是解决 CDH 困难问题，下面来详细描述 C 如何利用 A_1 来计算出 abP。

系统初始化阶段：挑战者 C 输入安全参数 λ，运行 setup 算法生成系统参数 *params*，其中 $P_{\text{Pub}}=aP$，然后将系统参数 *params* 发给 A_1。

询问阶段。为避免冲突，C 在此过程中维护以下 4 个列表 H_0^{list}、H_1^{list}、H_2^{list} 和 PK^{list}，起初全部为空。A_1 能够自适应地向 C 发起以下询问。

1) 用户生成询问。C 维护一个为空的 PK^{list} 列表，表中记录为 (ID_i,Q_i,D_i,x_i,X_i)。A_1 能够通过输入 ID_i 执行该用户生成询问，为了返回 A_1 的询问，C 随机选择数 $t\in\{1,2,\cdots,q_C\}$。当 A_1 输入 $ID_i(i\in[1,q_C])$，C 首先查询 PK^{list} 列表，如果列表中已经存在 (ID_i,Q_i,D_i,x_i,X_i)，则返回 (Q_i,X_i)。否则，C 将执行以下操作。

①若 $i\neq t$，C 随机选择 $\alpha_i,x_i\in Z_q^*$，令 $Q_i=\alpha_iP$，$D_i=\alpha_i(aP)$，$X_i=x_iP$，其中，x_i 为秘密值。

②若 $i=t$，C 随机选择 $\alpha_t,x_t\in Z_q^*$，令 $Q_t=bP-\alpha_tP$，$D_i=\perp$（符号 $\perp$ 表示该值未知），$X_t=x_tP$，其中，x_i 为秘密值。

以上 2 种情况中，C 将 (ID_i,Q_i,D_i,x_i,X_i) 添加到 PK^{list} 列表中，然后返回 (Q_i,X_i) 给 A_1。

2) 部分私钥提取询问。当 A_1 输入 $ID_i(i\in[1,q_{PPK}])$，C 首先查询 PK^{list} 列表，如果列表中没有 (ID_i,Q_i,D_i,x_i,X_i)，则 C 输出“$\perp$”。否则，C 执行

以下操作。

①若 $i \neq t$，C 返回 D_i。

②若 $i = t$，C 放弃并终止。

3) 秘密值询问。当 A_1 输入 $ID_i (i \in [1, q_{SV}])$，C 首先查询 PK^{list} 列表，如果列表中没有 $(ID_i, Q_i, D_i, x_i, X_i)$，$C$ 将输出“⊥”。否则，C 执行以下操作。

①若 $i \neq t$，C 返回 x_i。

②若 $i = t$，C 放弃并终止。

4) 公钥替换询问。当 C 收到一个关于 ID_i 的公钥 X_i 替换成 X_i' 询问时，C 首先查询 PK^{list} 列表，如果列表中存在 $(ID_i, Q_i, D_i, x_i, X_i)$，则 C 更新 X_i 为新的 X_i'；否则，C 将输出“⊥”。

5) H_1 询问。C 维护一个为空的列表 H_1^{list}，列表中的记录为 (Δ_i, β_i, H_i)。当 A_1 输入 $\Delta_i (i \in [1, q_{H_1}])$，$C$ 首先查询 H_1^{list} 列表，如果列表 H_1^{list} 中没有 (Δ_i, β_i, H_i)，C 随机选择 $\beta_i \in Z_q^*$，并计算 $H_i = \beta_i (aP)$，增加 (Δ_i, β_i, H_i) 至列表 H_1^{list} 中，返回 H_i 给 A_1；否则，C 返回 H_i。

6) H_2 询问。C 维护一个为空的列表 H_2^{list}，列表中的记录为 $(m_i, ID_i, X_i, \Delta_i, h_i)$。当 A_1 输入 $(m_i, ID_i, X_i, \Delta_i) (i \in [1, q_{H_2}])$，$C$ 首先查询 H_2^{list} 列表，如果列表 H_2^{list} 中已存在 $(m_i, ID_i, X_i, \Delta_i, h_i)$，则直接返回 h_i；否则 C 将执行以下操作。

①若 $ID_i \neq ID_t$，C 随机选择 $h_i \in Z_q^*$，输出 $(m_i, ID_i, X_i, \Delta_i, h_i, p_i = \perp)$ 并添加到列表 H_2^{list} 中。

②若 $ID_i = ID_t$，C 随机选择 $h_i \in Z_q^*$ 并掷币决定 p_i 的取值；其中，$p_i \in \{0,1\}$ $(Pr[p_i = 0] = \delta,\ Pr[p_i = 1] = 1 - \delta)$。

以上 2 种情况中，C 将 $(m_i, ID_i, X_i, \Delta_i, h_i, p_i)$ 添加到 H_2^{list} 列表中，然后返回 h_i 给 A_1。

7) 超级签名询问。当 A_1 输入某一个签名询问 $(m_j, ID_k) (k \in [1, q_S])$，$C$ 首先查询 PK^{list} 列表，如果列表中没有 $(ID_k, Q_k, D_k, x_k, X_k)$，$C$ 将输出“⊥”；否则，C 执行 (m_j, ID_k) 所对应的 PK^{list}、H_1^{list}、H_2^{list} 列表。

①若 $ID_k \neq ID_t$，C 随机选择 $x_i \in Z_q^*$ 并生成签名 $\sigma_i = (R_i, T_i)$。其中，$R_i = r_i P$，$T_i = h_i D_k + (x_i h_i + r_i) \beta_i (aP)$。

②若 $ID_k = ID_t$ 且 $p_i = 0$，C 生成签名 $\sigma_i = (R_i, T_i)$。其中，$R_i = -\beta_i^{-1} h_i (bP)$，$T_i = h_i \alpha_t aP + \beta_i h_i x_t (aP)$。

③若 $ID_k = ID_t$ 且 $p_i = 1$，C 放弃并终止。

伪造阶段。结束上述询问后，A_1 输出一个四元组 (m^*, ID^*, R^*, T^*)，其中，$m^* = (m_1^*, m_2^*, \cdots, m_n^*)$，$ID^* = (ID_1^*, ID_2^*, \cdots, ID_n^*)$，$(R^*, T^*)$ 为 n 个身份为 $ID_i^* (i = 1, 2, \cdots, n)$ 的用户 $U_i^* (i = 1, 2, \cdots, n)$ 分别对 n 个不同的消息 $m_i^* (i = 1, 2, \cdots, n)$ 生成的 n 个签名 (R_i^*, T_i^*) $(i = 1, 2, \cdots, n)$ 的聚合签名。根据假设，由于签名 $\sigma^* = (R^*, T^*)$ 是有效的，故 A_1 能赢得游戏。如果 $ID^* \neq ID_t$，C 放弃并终止。否则当 $ID^* = ID_t$ 时，C 执行以下步骤。

1) 若 $p^* = 0$，C 放弃并终止。

2) 若 $p^* = 1$，C 依靠 A_1 的伪造来解决 CDH 困难问题。

由于 A_1 生成一个有效签名 σ^*，伪造的聚合签名必须满足 $R^* = \beta^{*-1} (h^* \alpha^* P + bP)$，$T^* = (h^* + 1) abP + \beta^* h^* x^* (aP)$。其中，$\alpha^*$、$X^*$ 从 PK^{list} 列表中获得，β^* 从 H_1^{list} 列表中获得，以及 h^* 从 H_2^{list} 列表中获得。最终，C 利用 σ^* 来解决 CDH 困难问题，并输出 $abP = (h^* + 1)^{-1} (T^* - \beta^* h^* x^* (aP))$。

C 成功解决 CDH 困难问题的实例的概率可转化为以下 3 个事件。

E_1：C 在游戏过程中没有终止退出。

E_2：A_1 通过游戏伪造了一个有效并且非平凡的聚合签名。

E_3：上述 E_2 事件发生，存在 $i \in [1, n]$ 能满足 $ID^* = ID_t$，并且 $p^* = 1$。

如果上述事件均发生，则 C 赢得游戏，即 C 成功的概率为 $Pr[\text{E}_1 \wedge \text{E}_2 \wedge \text{E}_3] = Pr[\text{E}_1] Pr[\text{E}_2 | \text{E}_1] \cdot Pr[\text{E}_3 | \text{E}_1 \wedge \text{E}_2]$，其中，$Pr[\text{E}_1] \geqslant \left(1 - \frac{1}{q_C}\right)^{q_{\text{PPK}} + q_{\text{SV}}} (1 - \delta)^{q_S}$，$Pr[\text{E}_2 | \text{E}_1] \geqslant \varepsilon$，$Pr[\text{E}_3 | \text{E}_1 \wedge \text{E}_2] \geqslant \frac{\delta}{q_C}$，并且 $\delta = \frac{1}{q_S + 1}$ 能使 $\delta (1 - \delta)^{q_S}$ 达到最大值，可得

$$\varepsilon' = Pr[C(P, aP, bP) \to abP] \geqslant \left(1 - \frac{1}{q_C}\right)^{q_{\text{PPK}} + q_{\text{SV}}} \left(1 - \frac{1}{q_S + 1}\right)^{q_S} \frac{1}{q_C (q_S + 1)} \varepsilon \tag{17}$$

定理 2 在随机预言机模型和 CDH 困难假设下，本文方案在第 2 类攻击者 A_2 的适应性选择消息、选择身份以及公钥替换攻击下是存在不可伪造的。

引理 2 在随机预言机模型下，如果存在一个敌手 A_2，他能够在时间 t 内以不可忽略的概率 ε 成功攻破本文的无证书聚合签名方案，那么，

存在一个这样的算法 C，能利用算法以概率 $\varepsilon' \geqslant \left(1-\frac{1}{q_C}\right)^{q_{\mathrm{PPK}}+q_{\mathrm{SV}}}\left(1-\frac{1}{q_{\mathrm{S}}+1}\right)^{q_{\mathrm{S}}}\frac{1}{(q_C(q_{\mathrm{S}}+1))\varepsilon}$ 在时间 $t'<t+O(3q_C+q_{H_1}+q_{H_2}+4q_{\mathrm{S}}+2n+1)t_{\mathrm{m}}$ 内解决 CDH 问题，其中，t_m 表示一个点乘运算。

针对第 2 类敌手 A_2 的证明过程类似于第 1 类敌手 A_1 的证明过程，鉴于篇幅有限，证明过程略。

5.2　安全性和效率对比

判断一个 CLAS 方案实用与否，主要依据安全性和效率 2 个方面。

如表 1 所示，对于本文方案，无论是第 1 类攻击者类型还是第 2 类攻击者类型都支持超级签名询问的安全模型。表 1 中，B_1 代表中代表正常攻击者；B_2 代表强攻击者；B_3 代表超级攻击者；√表示方案中的攻击者所属类型；W 表示在该攻击者类型下方案的安全性程度较弱；S 表示在该攻击者类型下方案的安全性程度较强；L 表示长度单位。在保证安全性的前提下，无证书聚合签名方案还需注意通信和计算代价。如表 2 所示，本文将所提方案与现有方案在单个签名、验证和聚合验证 3 个方面进行详

表 1　　**安全性和通信代价对比**

方案	第 1 类				第 2 类				公钥长度	聚合签名长度
	B_1	B_2	B_3	安全性	B_1	B_2	B_3	安全性		
文献[31]CAS-1		√		W	√			W	2L	(n+1)L
文献[31]CAS-2		√		W	√			W	2L	2L
文献[32]			√	S	√			W	L	(n+1)L
文献[33]			√	S	√			W	L	2L
文献[34]			√	S			√	W	L	L
文献[35]			√	S			√	S	L	2L
文献[36]		√		W	√			W	L	(n+1)L
文献[37]			√	S			√	W	L	(n+1)L
文献[38]			√	S	√			W	L	(n+1)L
文献[39]			√	S	√			W	L	(n+1)L
文献[40]算法 1			√	S	√			W	L	2L
文献[40]算法 2			√	S			√	S	3L	2L
文献[28]			√	S	√			W	L	(n+1)L
本文方案			√	S			√	S	L	2L

表 2　　**效率对比**

方案	单个签名	验证	聚合验证
文献[31]CAS-1	2PM+1MTP+1PA	3P+2MTP	$(2n+1)\mathrm{P}+2n\mathrm{MTP}$
文献[31]CAS-2	2MTP+3GM+2PA	3PT+3MTP+1GM+1PA	$(n+2)\mathrm{P}+(2n+1)\mathrm{MTP}+n\mathrm{GM}+n\mathrm{PA}$
文献[32]	3PM+2MTP+2PA	4P+3MTP	$(n+3)\mathrm{P}+(2n+1)\mathrm{MTP}$
文献[33]	5PM+3MTP+4PA+1H	5P+4MTP+2PM+1PA+1H	$5P+(n+3)\mathrm{MTP}+n\mathrm{H}+2n\mathrm{PM}+n\mathrm{PA}$
文献[34]	3PM+3ZM+1PA+1H	3P+2MTP+3PM+1PA+3H	$3\mathrm{P}+2n\mathrm{MTP}+3n\mathrm{PM}+3n\mathrm{H}+n\mathrm{PA}$
文献[35]	5PM+3ZM+3PA+1H	4P+2MTP+3PM+2PA+3H	$4\mathrm{P}+2n\mathrm{MTP}+3n\mathrm{PM}+2n\mathrm{PA}+3n\mathrm{H}$
文献[36]	4ZM+2H	3P+1MTP+1ZM+1H	$(n+2)\mathrm{P}+n\mathrm{MTP}+n\mathrm{ZM}+n\mathrm{H}$
文献[37]	3PM+2ZM+1H	3P+1MTP+2PM+1H+1PA	$3\mathrm{P}+n\mathrm{MTP}+2n\mathrm{PM}+n\mathrm{H}+n\mathrm{PA}$
文献[38]	3PM+2ZM+2H+2PA	3P+1MTP+2PM+2H+1PA	$3\mathrm{P}+n\mathrm{MTP}+2n\mathrm{PM}+2n\mathrm{H}+n\mathrm{PA}$
文献[39]	3PM+2MTP+2ZM+2H+2PA	4P+3MTP+2PM+2H	$4\mathrm{P}+(n+2)\mathrm{MTP}+2n\mathrm{PM}+2n\mathrm{H}$
文献[40]算法 1	5E+1PM+2MTP+3GM+2H	4P+4MTP+1GM+2E+2H	$4\mathrm{P}+(2n+2)\mathrm{MTP}+n\mathrm{GM}+2n\mathrm{E}+2n\mathrm{H}$
文献[40]算法 2	3E+1MTP+1GM+1ZM+1H	4P+2MTP+1E+1H	$(n+3)\mathrm{P}+2n\mathrm{MTP}+n\mathrm{E}+n\mathrm{H}$
文献[28]	4PM+1MTP+2ZM+1H+4PA	3P+2MTP+2PM+1H+2PA	$3\mathrm{P}+(n+1)\mathrm{MTP}+2n\mathrm{PM}+n\mathrm{H}+2n\mathrm{PA}$
本文方案	1PM+1H+1PA	3P+2MTP+2PM+1H+1PA	$3\mathrm{P}+(n+1)\mathrm{MTP}+2n\mathrm{PM}+n\mathrm{H}+n\mathrm{PA}$

细的对比，所用运算符号见表 3。不难发现，本文的方案在效率方面相对较高。

表 3 符号定义

符号	定义
ZM	Z_q^* 上执行一次乘法运算
GM	群上执行一次乘法运算
H	执行一次散列函数
E	执行一次指数运算
P	执行一次双线性对运算
PM	执行一次椭圆曲线上点乘运算
MTP	执行一次 Maptopoint 函数
PA	执行一次椭圆曲线上点加运算

6 基于无证书聚合签名的匿名漫游认证方案

本文具有隐私保护的匿名漫游认证方案，主要包含 3 个阶段：系统初始化、漫游认证以及聚合验证。所使用的相关符号，如表 4 所示。

6.1 系统初始化

本文所提方案的系统初始化详细过程，如图 4 所示。

6.2 匿名漫游认证

本节描述 MN 移动到 FA 所负责的网络范围内进行匿名漫游认证的详细过程，如图 5 所示，该过程主要由 MN 和 FA 完成。

表 4 相关符号

符号	定义
ID_N	实体 N 的身份信息
pid_i	MN 的一个别名
$Date_{pid_i}$	pid_i 的有效期
$f(x,y)$	有限域 F_q 上的二维多项式
RPL	注销别名列表
D_{pid_i}	pid_i 的部分私钥（基于 CLAS 算法）
x_{pid_i}	pid_i 的秘密值（基于 CLAS 算法）
PK_{pid_i}	pid_i 的公钥（基于 CLAS 算法）
SK_{pid_i}	pid_i 的完整私钥（基于 CLAS 算法）
σ_N	实体 N 的签名
tt_i	时间戳
$K_{\text{MN-FA}}$	MN 和 FA 的共享密钥
MAC	认证码
MAC'	新的认证码
E_{PK}	公钥（基于 ECDSA 算法）
E_{SK}	私钥（基于 ECDSA 算法）

6.3 聚合验证

在实际生活中，多个 MN 来自同一个家乡网络，有可能 n 个 MN 同时向服务器 HA 或 FA 发出接入请求。在漫游认证过程中，签名验证的计算开销直接影响服务器的总体开销，因此，本文设计了一种聚合验证方法，使服务器可以一次批量验证多个 MN 的签名（如图 6 所示），大大降低了签名验证的计算开销。

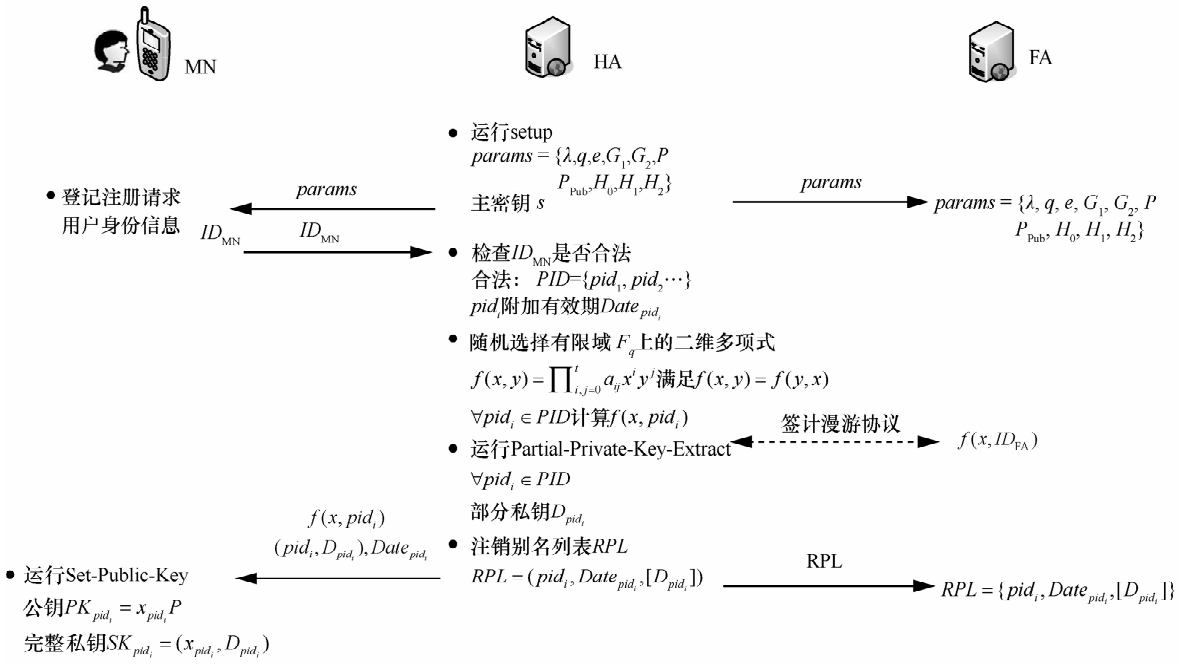

图 4 系统初始化详细步骤

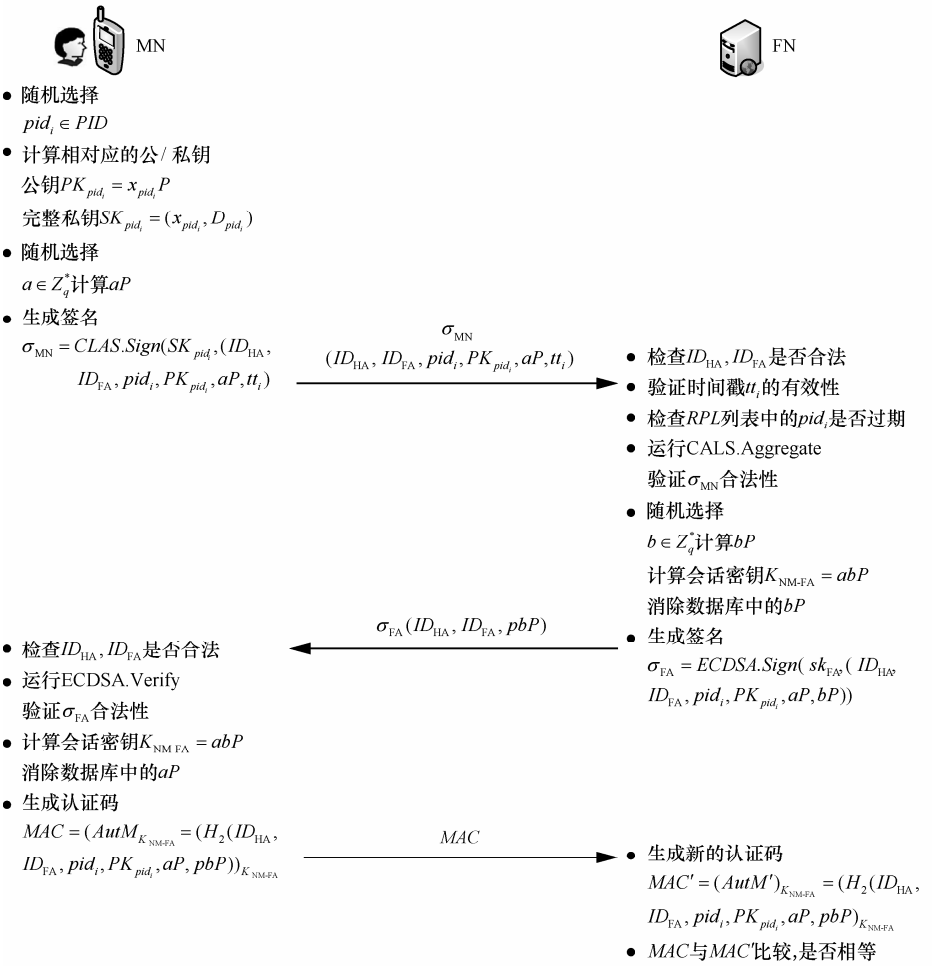

图 5　匿名漫游认证过程和会话密钥建立的详细步骤

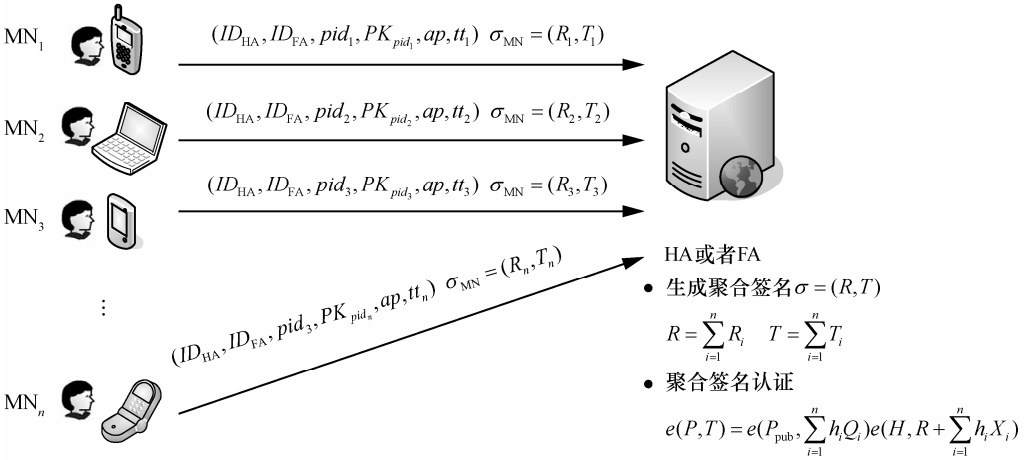

图 6　聚合验证

7　性能评估

7.1　安全性对比

将本方案与近几年相关文献中的方案分别在安全需求和攻击类型 2 方面进行对比，如表 5 和表 6 所示。表 5 中√表示能实现该性质；×表示不能上实现该性质；W 表示该性质较弱；S 表示该性质较强。表 6 中√表示能解决该问题或能抵抗该攻击；×表示不能解决该问题或无法抵抗该攻击；W 表示该抵抗该攻击能力较弱；S 表示抵抗该攻击能力较强。

表 5　　**安全需求对比**

方案	动态撤销	会话密钥	隐匿性和不可追踪性	条件隐私保护	密码学方法
文献[12]	×	S	W	√	PKI
文献[16]	×	S	S	√	ID-PKC
文献[17]	√	S	W	×	GS
文献[6]	×	W	W	√	对称密钥
文献[21]	√	S	S	×	GS
文献[22]	√	W	S	√	ID-PKC
文献[25]	×	S	W	×	对称密钥
文献[24]	√	W	S	√	ID-PKC
文献[26]	×	S	W	×	对称密钥
本文方案	√	S	S	√	CL-PKC

表 6　　**攻击类型对比**

方案	密钥托管	DoS 攻击		重放攻击	伪造攻击	Deposit-case 攻击	被动偷听攻击
		情况 1	情况 2				
文献[12]	×	√	×	√	√	×	W
文献[16]	×	√	×	√	√	√	S
文献[17]	×	√	×	√	√	√	S
文献[6]	×	√	×	√	√	×	W
文献[21]	×	√	×	√	√	√	S
文献[22]	×	√	√	√	√	√	W
文献[25]	×	×	×	×	√	×	W
文献[24]	×	√	×	√	√	√	S
文献[26]	×	√	×	√	√	×	W
本文方案	√	√	√	√	√	√	S

可见本文的方案能满足所述的全部安全需求，避免了密钥托管问题，并且有较强的攻击抵御性，使安全性大大提高。

7.2　效率对比

漫游认证过程中，除了要保证较高的安全性外，也要注重效率问题。MN 在漫游认证整个过程中一直处于连接状态，因而通信开销应尽量小，另外，MN 计算能力是有限的，所以要保证计算开销较低。假设 MN 与 FA 交互时的传输开销为 α ms。本文将所提方案与同样采用两方漫游认证的现有方案进行对比，结果如表 7 所示，其中，计算开销所用符号可参见表 3。不难看出，本文的方案通信开销和计算开销较小，效率高，实用性强。

表 7　　**效率对比**

方案	参与方数量	聚合验证（或批验证）	通信开销/ms	MN 所消耗计算开销
文献[17]	2	×	3α	3P +11E
文献[21]	2	×	3α	1P+7E
文献[22]	2	√	2α	2MTP+2H+1PM
文献[24]	2	√	2α	2MTP+2H+3PM
本文方案	2	√	3α	1H+4PM

8　结束语

针对无线网络中的漫游认证问题，本文构造了一个无证书的聚合签名方案，通过对该方案的安全性和效率分析，易知本文签名方案在签名和验证过程中，无论是单个验证还是聚合验证所需要的计算开销都较少，适用于计算和存储有限的移动设备。在此基础上，提出了无线网络中具有隐私保护的匿名漫游认证方案，满足用户隐匿性、不可追踪性等安全需求，抵抗重放攻击、DoS 攻击等，也避免了密钥托管问题。另外，本文方案中 MN 所耗计算开销较少，FA 利用聚合技术能够同时验证多个用户签名，加快了认证速度，同时减少了通信和计算代价。在未来的工作里，如何在满足隐私保护和安全的基础上，解决恶意用户拒绝付费的问题是下一步将要探究的问题。

参考文献：

[1] TZENG Z J, TZENG W G. Authentication of mobile users in third generation mobile systems[J]. Wireless Personal Communications, 2001, 16(1): 35-50.

[2] HWANG K F, CHANG C C. A self-encryption mechanism for authentication of roaming and teleconference services[J]. IEEE Transactions on Wireless Communications, 2003, 2(2): 400-407.

[3] JIANG Y, LIN C, SHEN X, et al. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks[J]. IEEE Transactions on Wireless Communications, 2006, 5(9): 2569-2577.

[4] ARKKO J, HAVERINEN H. Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA)[J]. Heise Zeitchriften Veriag, 2006, 47(2): 64-77.

[5] CHANG C C, LEE C Y, CHIU Y C. Enhanced authentication scheme with anonymity for roaming service in global mobility networks[J]. Computer Communications, 2009, 32(4): 611-618.

[6] ZHOU T, XU J. Provable secure authentication protocol with anonymity for roaming service in global mobility networks[J]. Computer Networks, 2011, 55(1): 205-213.

[7] GO J, PARK J, KIM K. Wireless authentication protocol preserving user anonymity[J]. Authentication, 2001, 3(2): 78-81.

[8] HE D, MA M, ZHANG Y, et al. A strong user authentication scheme with smart cards for wireless communications[J]. Computer Communications, 2011, 34(3): 367-374.

[9] REN K, LOU W, KIM K, et al. A novel privacy preserving authentication and access control scheme for pervasive computing environments[J]. IEEE Transactions on Vehicular Technology, 2006, 55(4): 1373-1384.

[10] TREVATHAN J, GHODOSI H, READ W. An anonymous and secure continuous double auction scheme[C]// The 39th Annual Hawaii International Conference on System Sciences. IEEE, c2006: 125.

[11] KIM J, CHOI S, KIM K, et al. Anonymous authentication protocol for dynamic groups with power-limited devices[C]//Symposium on Cryptography and Information Security (SCIS'03). c2013: 405-410.

[12] YANG G, WONG D S, DENG X. Anonymous and authenticated key exchange for roaming networks[J]. IEEE Transactions on Wireless Communications, 2007, 6(9): 3461-3472.

[13] YANG G, WONG D S, DENG X. Formal security definition and efficient construction for roaming with a privacy-preserving extension[J]. JUCS, 2008, 14(3): 441-462.

[14] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8): 1271-1281.
PENG H X. An identity-based authentication model for multi-domain[J]. Chinese Journal of Computers, 2006, 29(8): 1271-1281.

[15] WAN Z, REN K, PRENEEL B. A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks[C]//The first ACM Conference on Wireless Network Security. ACM, c2008: 62-67.

[16] FATEMI M, SALIMI S, SALAHI A. Anonymous roaming in universal mobile telecommunication system mobile networks[J]. IET Information Security, 2010, 4(2): 93-103.

[17] YANG G, HUANG Q, WONG D S, et al. Universal authentication protocols for anonymous wireless communications[J]. IEEE Transactions on Wireless Communications, 2010, 9(1): 168-174.

[18] 田子建, 王继林, 伍云霞. 一个动态的可追踪匿名认证方案[J]. 电子与信息学报, 2005, 27(11): 1737-1740.
TIAN Z J, WANG J L, WU Y X. A dynamic traceable anonymous authentication scheme[J]. Journal of Electronics & Information Technology, 2005, 27(11): 1737-1740.

[19] HOU H, LIU S. CPK-based authentication and key agreement protocols with anonymity for wireless network[C]//2009 International Conference on Multimedia Information Networking and Security. IEEE, c2009: 347-350.

[20] ZHANG M, PEI C, DANG L. An efficient certificateless registration protocol for mobile IP networks[J]. Journal of Convergence Information Technology, 2012, 7(23): 34-41.

[21] HE D, BU J, CHAN S, et al. Privacy-preserving universal authentication protocol for wireless communications[J]. IEEE Transactions on Wireless Communications, 2011, 10(2): 431-436.

[22] HE D, CHEN C, CHAN S, et al. Secure and efficient handover authentication based on bilinear pairing functions[J]. IEEE Transactions on Wireless Communications, 2012, 11(1): 48-53.

[23] HE D, CHEN C, CHAN S, et al. Analysis and improvement of a secure and efficient handover authentication for wireless networks[J]. Communications Letters, IEEE, 2012, 16(8): 1270-1273.

[24] TSAI J L, LO N W, WU T C. Secure handover authentication protocol based on bilinear pairings[J]. Wireless Personal Communications, 2013, 73(3): 1037-1047.

[25] KIM J S, KWAK J. Improved secure anonymous authentication scheme for roaming service in global mobility networks[J]. International Journal of Security and Its Applications, 2012, 6(3): 45-54.

[26] KUO W C, WEI H J, CHENG J C. Enhanced secure authentication scheme with anonymity for roaming in mobility networks[J]. Information Technology and Control, 2014, 43(2): 151-156.

[27] ZHANG Y, WANG C. Comment on new construction of efficient certificateless aggregate signatures[J]. International Journal of Security and Its Applications, 2015, 9(1): 147-154.

[28] CHENG L, WEN Q, JIN Z, et al. Cryptanalysis and improvement of a certificateless aggregate signature scheme[J]. Information Sciences,

2015, 295: 337-346.

[29] CHEN Y C, TSO R, HORNG G, et al. Strongly secure certificateless signature: cryptanalysis and improvement of two schemes[J]. Journal of Information Science and Engineering, 2015, 31(1): 297-314.

[30] HUANG X, MU Y, SUSILO W, et al. Certificateless signature revisited[C]//Information Security and Privacy. Springer Berlin Heidelberg, c2007: 308-322.

[31] GONG Z, LONG Y, HONG X, et al. Two certificateless aggregate signatures from bilinear maps[C]//Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, c2007: 188-193.

[32] ZHANG L, ZHANG F. A new certificateless aggregate signature scheme[J]. Computer Communications, 2009, 32(6): 1079-1085.

[33] ZHANG L, QIN B, WU Q, et al. Efficient many-to-one authentication with certificateless aggregate signatures[J]. Computer Networks, 2010, 54(14): 2482-2491.

[34] XIONG H, WU Q, CHEN Z. Strong security enabled certificateless aggregate signatures applicable to mobile computation[C]//2011 Third International Conference on Intelligent Networking and Collaborative Systems (INCoS). IEEE, c2011: 92-99.

[35] XIONG H, WU Q, CHEN Z. An efficient provably secure certificateless aggregate signature applicable to mobile computation[J]. Control and Cybernetics, 2012, 41(2): 373-391.

[36] CHEN Y C, HORNG G, LIU C L, et al. Efficient certificateless aggregate signature scheme[J]. Journal Electronic Science and Technology, 2012, 10: 209-214.

[37] XIONG H, GUAN Z, CHEN Z, et al. An efficient certificateless aggregate signature with constant pairing computations[J]. Information Sciences, 2013, 219(10): 225-235.

[38] LIU H, WANG S, LIANG M, et al. New construction of efficient certificateless aggregate signatures[J]. International Journal of Security and Its Applications, 2014, 8: 411-422.

[39] TU H, HE D, HUANG B. Reattack of a certificateless aggregate signature scheme with constant pairing computations[J]. The Scientific World Journal, 2014, 2014(9-10): 343715.

[40] 刘贺. 移动网络接入认证的隐私保护研究[D]. 北京: 北京交通大学, 2014.
LIU H. Research on privacy protection in access authentication for mobile networks[D]. Beijing: Beijing Jiaotong University, 2014.

作者简介：

刘丹（1991-），女，安徽马鞍山人，安徽大学硕士生，主要研究方向为网络与信息安全。

石润华（1974-），男，安徽安庆人，安徽大学教授、博士生导师，主要研究方向为无线网络安全、保护隐私的多方协作计算、可证明安全的量子密码。

张顺（1982-），男，安徽安庆人，安徽大学副教授、硕士生导师，主要研究方向为信息计算复杂性、高振荡问题易处理性和量子计算。

仲红（1965-），女，安徽固镇人，安徽大学教授、博士生导师，主要研究方向为无线传感网、安全多方计算、私有信息保护。